INFO-0126

ACNS Advisory Committee on Nuclear Safety
CCSN Comité consultatif de la sûreté nucléaire

ACNS-7

REPORT ON AECB CONSULTATIVE DOCUMENT C-70 "THE USE OF FAULT TREES IN LICENSING SUBMISSIONS"

by the

Advisory Committee on
Nuclear Safety

January 1984

Committee Reports

Since the 1950's the Atomic Energy Control Board has made use of advisory committees of independent experts to assist it in its decision-making process. In 1979 the Board restructured the organization of these consultative groups, resulting in the creation of two senior level scientific committees charged with providing the Board with independent advice on principles, standards and general practices related to radiation protection and the safety of nuclear facilities. The two committees are the Advisory Committee on Radiological Protection (ACRP), formed in 1979, and the Advisory Committee on Nuclear Safety (ACNS), which was established a year later. Summaries of meetings of the committees are available to the public in the AECB library in Ottawa.

From time to time the committees issue reports which are normally published by the AECB and catalogued within the AECB's public document system. Committee reports, bound with a distinctive cover, carry both a committee-designated reference number, e.g. ACRP-1, and an AECB reference number in the "INFO" series. The reports generally fall into two broad categories: (i) recommendations to the Board on a particular technical topic, and (ii) background studies. Unless specifically stated otherwise, publication by the AECB of a committee report does not imply endorsement by the Board of the content, nor acceptance of any recommendations made therein.

ACNS Report on AECB Consultative Document C-70
"The Use of Fault Trees in Licensing Submissions"

Introduction

The Atomic Energy Control Board (AECB) has issued Consultative Document C-70, "The Use of Fault Trees in Licensing Submissions", for public comment. The Advisory Committee on Nuclear Safety (ACNS) has examined this document and ACNS members have met with AECB staff and representatives of the nuclear industry to discuss it. The ACNS presents its comments and recommendations in this report.

Objective and Scope of C-70

The objective of the proposed regulatory guide "The Use of Fault Trees in Licensing Submissions", as stated in section 1.2 of Consultative Document C-70 is:

"... to standardize the fault tree presentation technique in order to:

(a) prevent errors in interpretation of fault trees, especially when the fault tree is used or reviewed by a person other than the originator of the fault tree.

(b) facilitate the use of computer facilities for fault tree processing."

The document defines a fault tree as a hierarchically-structured graphical representation of system failures and their potential causes.

The document then states certain basic characteristics or attributes which fault trees should possess, and certain conditions affecting the use of fault trees. It defines fault tree fundamentals, sets criteria for the application of fault trees to systems and defines ground rules for a fault tree format. Finally, in two appendices, it includes specific rules for fault tree symbols and fault tree description files for computer use. The appendices are referred to in the text as "acceptable" standards or methods.

Background

The first version of C-70, in which the appendices were cited as mandatory requirements, was transmitted to the ACNS for its information and consideration on May 3, 1982.(1) At the 13th meeting of ACNS on June 25, 1982, certain members expressed concern that the approach contained in C-70 was a departure from the AECB practice in reactor regulation of specifying objectives and general requirements rather than detailed procedures. An expression of this concern was contained in a memorandum issued on behalf of the ACNS in November, 1982.(2)

A slightly modified version of C-70 was issued for public comment as a proposed regulatory guide on May 31, 1983. At its meeting on June 27, 1983, the ACNS requested the Working Group on ACNS-4 to prepare a formal response to document C-70. The membership of the Working Group is shown in Annex 1.

The Working Group met with members of the AECB staff involved with C-70 on three occasions and with representatives of Ontario Hydro and Atomic Energy of Canada Limited (AECL), CANDU Operations, to discuss C-70 and its implications.

Based on information received in these meetings and from a study of various relevant documents, the Working Group developed recommendations on C-70 which were presented to the ACNS at its meeting of December 15, 1983. The ACNS endorsed these recommendations in principle and issued this report, which was approved at its meeting of January 23, 1984.

Response of the Nuclear Industry to C-70 and AECB Reactions to This Response

Ontario Hydro and AECL CANDU Operations representatives objected to the approach taken in C-70, as contained in the first version issued in May, 1982, as being a significant departure from the existing Canadian practice in nuclear reactor regulation and licensing of stating objectives and general requirements rather than specifying detailed procedures. There was considerable concern that acceptance of C-70 would set a "dangerous precedent" for reactor regulation in Canada. Also, these organizations pointed out that fault tree methodology is only one tool in reactor reliability analysis and that C-70 might detract from the use of other methods that might be more appropriate in many cases. The industry representatives recommended that, rather than issuing C-70, priority should be given to the drafting of a CSA standard by the existing CSA Working Group, N290.9, (on which the AECB is represented) on reliability analysis of safety-related systems of CANDU nuclear power plants.

Industry responses also included a number of specific objections to, and criticisms of, the material in C-70.

In reaction to the industry response, AECB staff, in the revised version of C-70 issued for public comment May 31, 1983, eliminated the mandatory nature of the Appendices and characterized them as acceptable standards and methods. Otherwise, there were no substantive changes between the initial version and the final version issued for public comment.

Ontario Hydro and AECL representatives reiterated their objections to the reissued version of C-70, and stated that their original positions had not been substantially modified by the revised version.

Assessment of Present Situation by the ACNS

In its first meeting with the AECB staff, the ACNS Working Group was given a comprehensive overview on the use of fault trees in licensing submissions. In particular, AECB staff identified a number of deficiencies in past practice in fault tree analysis by licensees and stated why they believed that C-70 was needed.

In subsequent meetings of the Working Group with AECL and Ontario Hydro, representatives of these organizations acknowledged that there had been weaknesses in past fault tree submissions but claimed that these had been, or were in the process of being, overcome and that C-70, if it had ever been needed, was no longer required.

In later meetings, AECB staff members agreed that there had been considerable improvement in fault tree submissions since May, 1982, when the first version of C-70 was issued, and that in many areas remaining differences were being resolved through normal licensing processes.

From these meetings, outstanding problems appear to be:

a) inadequate identification of specific components, particularly in redundant systems and in safety support systems, and their modes of failure, in the various fault trees submitted;

b) an insufficient clarity and generality of submissions to permit and facilitate reliable auditing by AECB staff;

c) the lack of adequate feed-back of operational experience to the designers to permit periodic up-dating of fault trees and risk estimates.

The ACNS understands that efforts are continuing between Board staff and licensees in an effort to overcome the first two of the above problems. Also, the ACNS has been informed that Ontario Hydro has made a commitment to update fault trees on an annual basis in the light of field experience to assist in overcoming the third problem.

The ACNS believes that C-70, in its original version and the revised version for public comment, has served a useful role in stimulating improvements in fault tree submissions by the licensees and in underlining the need for a CSA standard in the area of reliability analysis for safety-related systems in CANDU reactors.

The ACNS also believes, however, that the issuance of C-70 as a Regulatory Guide, even in its present form with the previously mandatory requirements of the Appendices modified to "acceptable" methods, still constitutes a significant departure from existing Canadian practice that would have implications beyond the immediate question of fault tree analysis. In its "Recommended General Safety Requirements for Nuclear Power Plants", ACNS-4[3], the ACNS has stated its support for the continuation of the existing Canadian practice in reactor regulation. Thus, the ACNS cannot support the significant break from past practice that would be represented by the issuing of C-70 as an AECB Regulatory Guide.

The ACNS recognizes, however, that there remains an urgent need for the establishment of a workable standard for reliability analysis for safety-related systems in CANDU reactors and strongly believes that the most effective means of establishing such a standard is through the existing CSA Working Group, N290.9. The ACNS urges that this approach be pursued as expeditiously as possible. The ACNS recognizes that, failing the early development of a CSA standard, AECB may have no option but to issue documents such as C-70, which the ACNS believes would be detrimental to the process of reactor regulation in Canada.

Recommendations of ACNS

The Advisory Committee on Nuclear Safety recommends:

1. that the present version of C-70 not be issued as a Regulatory Guide.

2. that AECB issue as a Regulatory Guide a statement of the general principles that effective fault tree analyses should follow, without any stipulation of detailed procedures. (However, the ACNS is not convinced that such a document will be necessary if recommendation (4) is implemented soon.)

3. that the licensees work diligently to resolve with the Board staff the remaining weaknesses in fault tree submissions, particularly those in the areas of:

   a) unequivocal identification of components and their failure modes;

   b) clarity and generality of submissions to permit reliable auditing by AECB staff;

   c) feed-back of operational experience to permit periodic updating of fault trees and risk estimates.

4. that the highest priority be given by licensees and AECB to the expeditious development, following normal procedures, of a CSA standard on Reliability Analysis of Safety-Related Systems in CANDU Nuclear Power Plants. The AECB must continue to be represented on the CSA Working Group developing this standard and the present version of C-70 should be used as one input to the development of this standard.

References

1. Boyd, F.C., AECB Consultative Document C-70: "Regulatory Guide on the Use of Fault Trees in Licensing Submissions" (undated). Memo to ACNS, May 3, 1982.

2. Boyd, F.C., ACNS Comments on C-70. Memo to R.J. Atchison, Nov. 29, 1982.

3. Recommended General Safety Requirements for Nuclear Power Plants. ACNS-4, June, 1983.

ANNEX 1

Members of the ACNS Working Group on Consultative Document C-70

J. T. Rogers, Chairman
N. C. Lind
O. R. Lundell
A. Pearson

F. C. Boyd, Secretariat

INFO-0126

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

CCSN-7

RAPPORT SUR LE DOCUMENT DE CONSULTATION C-70 DE LA CCEA : "L'UTILISATION DES ARBRES DE DÉFAILLANCES POUR LA PRÉSENTATION DES DEMANDES DE PERMIS"

par le

Comité consultatif de la sûreté nucléaire

janvier 1984

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

RAPPORTS DES COMITÉS

Depuis les années 1950, la Commission de contrôle de l'énergie atomique a recours à des comités consultatifs composés d'experts indépendants pour l'aider dans ses prises de décision. En 1979, la CCEA a restructuré l'organisation de ces groupes de consultation pour former deux comités scientifiques supérieurs chargés de lui fournir des conseils indépendants à l'égard des principes, des normes et des méthodes générales touchant la radioprotection et la sûreté des installations nucléaires: ce sont le Comité consultatif de la radioprotection (CCRP), formé en 1979, et le Comité consultatif de la sûreté nucléaire (CCSN), établi l'année suivante. Le public peut consulter les comptes rendus des réunions des comités à la bibliothèque de la CCEA, à Ottawa.

De temps en temps, les comités préparent des rapports qui sont normalement publiés par la CCEA et catalogués dans la collection des documents publics de la CCEA. Reliés sous une couverture particulière, les rapports des comités sont identifiés par un numéro de référence attribué par le comité d'origine, comme CCRP-1, et par un numéro de référence donné par la CCEA dans la série "INFO". Les rapports se divisent habituellement en deux catégories générales: (i) recommandations présentées à la Commission concernant un sujet d'ordre technique particulier, et (ii) études générales. À moins d'indication contraire, toute publication d'un rapport de comité effectuée par la CCEA ne signifie pas que la Commission approuve le contenu de la publication, ni qu'elle accepte les recommandations qui y sont faites.

Rapport sur le document de consultation C-70 de la CCEA : "L'Utilisation des arbres de défaillances pour la présentation des demandes de permis"

INTRODUCTION

La Commission de contrôle de l'énergie atomique (CCEA) a publié pour commentaires le document de consultation C-70 intitulé "L'Utilisation des arbres de défaillances pour la présentation des demandes de permis". Le Comité consultatif de la sûreté nucléaire (CCSN) a examiné le document et les membres du CCSN ont rencontré certains spécialistes de la CCEA et des représentants de l'industrie nucléaire pour en discuter. Le présent rapport fait état des commentaires et des recommandations du CCSN.

OBJECTIF ET PORTÉE DU DOCUMENT C-70

L'objectif du projet de guide de réglementation intitulé "L'Utilisation des arbres de défaillances pour la présentation des demandes de permis" est défini à l'article 1.2 du document de consultation C-70 :

"[. . .] normaliser la technique de présentation de l'arbre de défaillances afin

a) d'éviter les erreurs d'interprétation surtout lorsque les arbres de défaillances sont utilisés ou examinés par une autre personne que leur créateur;

b) de faciliter l'utilisation de l'ordinateur dans le traitement des arbres de défaillances."

Le document définit l'arbre de défaillances comme une représentation graphique et hiérarchique des défaillances d'un système et de leurs causes probables.

Le document traite ensuite de certaines caractéristiques fondamentales que tout arbre de défaillances devrait comporter, de même que certaines conditions afférentes à l'utilisation des arbres de défaillances. Il définit les aspects fondamentaux des arbres de défaillances, en établit les critères d'application aux différents systèmes et en fournit les grandes lignes de présentation. Enfin, deux annexes donnent des règles particulières sur les symboles et les fichiers de description des arbres de défaillances à utiliser en informatique. Les normes ou les méthodes recommandées dans les annexes sont considérées comme "acceptables" dans le texte.

HISTORIQUE

La première version du document C-70 dans lequel les annexes constituaient des exigences réglementaires a été transmise au CCSN pour information et commentaires, le 3 mai 1982 (1). Lors de la treizième réunion du CCSN, le 25 juin 1982, quelques membres ont exprimé leur inquiétude quant à l'approche du document C-70, qui s'écartait de la pratique de la CCEA d'identifier certains objectifs et certaines exigences générales plutôt que d'imposer des marches à suivre détaillées pour réglementer les réacteurs. Une note de service envoyée en novembre 1982 au nom du CCSN faisait part de cette inquiétude (2).

Une version légèrement modifiée du document C-70 a été publiée pour commentaires, le 31 mai 1983, comme projet de guide de réglementation. Lors de sa réunion du 27 juin 1983, le CCSN a demandé au Groupe de travail du CCSN-4 de préparer une réponse officielle au document C-70. Le nom des membres du groupe de travail apparaît à l'annexe 1.

Le groupe de travail a rencontré les spécialistes de la CCEA responsables du document C-70 à trois reprises et certains représentants d'Ontario Hydro et des Opérations CANDU de L'Énergie atomique du Canada, Limitée (L'EACL) pour discuter du document C-70 et de ses répercussions.

D'après les données obtenues à la suite de ces réunions et d'une étude des différents documents pertinents, le Groupe de travail a mis au point certaines recommandations sur le document C-70 qu'il a présentées au CCSN lors de sa réunion du 15 décembre 1983. Le CCSN a donné son accord de principe à ces recommandations et a publié le présent rapport qu'il a approuvé à sa réunion du 23 janvier 1984.

RÉPONSE DE L'INDUSTRIE NUCLÉAIRE AU DOCUMENT C-70
ET RÉACTION DE LA CCEA

Les représentants d'Ontario Hydro et des Opérations CANDU de L'EACL se sont opposés à l'approche du document C-70, telle qu'elle apparaissait dans la première version publiée en mai 1982, comme étant un écart important par rapport à la pratique canadienne actuelle en matière d'autorisation et de réglementation des réacteurs nucléaires, qui consiste à identifier certains objectifs et certaines exigences générales plutôt que d'imposer des marches à suivre détaillées. On craint fort notamment que l'approbation du document C-70 établirait un "précédent dangereux" en réglementation des réacteurs au Canada. Par ailleurs, ces organismes ont signalé que les arbres de défaillances ne représentaient qu'une méthode d'analyse de fiabilité des réacteurs et que l'application du document C-70 pourrait décourager le recours à d'autres méthodes appropriées dans plusieurs cas. Les représentants de l'industrie ont recommandé d'accorder la priorité à l'ébauche d'une norme de l'ACNOR par le Groupe de travail actuel de l'ACNOR N290.9 sur les analyses de fiabilité des systèmes liés à la sûreté des centrales nucléaires CANDU, dont la CCEA fait partie, plutôt que de publier le document C-70 comme document de réglementation. L'industrie a également fait part de certaines objections et critiques particulières relatives au contenu du document C-70.

En réponse aux observations de l'industrie, les spécialistes de la CCEA ont abrogé le statut obligatoire des annexes et les ont plutôt identifiées comme des normes et des méthodes acceptables dans la version modifiée du document C-70 publiée pour commentaires le 31 mai 1983. Sauf pour cette modification, la version originale et la version finale publiée pour commentaires sont essentiellement les mêmes.

Les représentants d'Ontario Hydro et de L'EACL ont réitéré leur opposition à la nouvelle publication du document C-70 et ont déclaré qu'ils n'avaient pas changé leur position originale de manière importante face à la version modifiée.

ÉVALUATION DE LA SITUATION ACTUELLE PAR LE CCSN

Au cours de sa première réunion avec les spécialistes de la CCEA, le Groupe de travail du CCSN a reçu un aperçu détaillé de l'utilisation des arbres de défaillances pour la présentation des demandes de permis. En particulier, les spécialistes de la CCEA ont identifié certaines lacunes des analyses précédentes au moyen d'arbres de défaillances par les titulaires de permis et ont expliqué pourquoi le document C-70 s'avérait nécessaire à leurs yeux.

Lors des réunions suivantes du Groupe de travail avec L'EACL et Ontario Hydro, les représentants de ces organismes ont reconnu que les présentations passées d'arbres de défaillances péchaient par certaines faiblesses, mais ont soutenu que celles-ci avaient été surmontées ou étaient sur le point de l'être et, par conséquent, que le document C-70 n'avait plus sa raison d'être, si jamais il en avait eu une.

Lors de réunions ultérieures, les spécialistes de la CCEA ont reconnu que les présentations d'arbres de défaillances s'étaient de beaucoup améliorées depuis la première version du document C-70, en mai 1982, et que, dans plusieurs domaines, les quelques différences en suspens étaient résolues au cours du processus normal d'autorisation.

À la suite de ces diverses réunions, il semble que les problèmes suivants restent à résoudre :

a) le manque d'identification adéquate des composants particuliers, notamment des systèmes redondants et des systèmes de sûreté auxiliaires, et de leurs modes de défaillance, dans la présentation des divers arbres de défaillances;

b) le manque de clarté et de vue d'ensemble dans les présentations afin d'en permettre et d'en faciliter une vérification fiable par les spécialistes de la CCEA; et

c) le manque de retour d'information adéquat aux concepteurs en matière d'expérience d'exploitation, afin de permettre la mise à jour périodique des arbres de défaillances et des calculs de risque.

Le CCSN comprend que les spécialistes de la CCEA et les titulaires de permis poursuivent leurs efforts pour surmonter les deux premiers problèmes. D'autre part, le CCSN a appris qu'Ontario Hydro s'est engagé à mettre à jour ses arbres de défaillances chaque année d'après l'expérience acquise sur le tas, dans son effort de collaboration pour surmonter le troisième problème.

Le CCSN est d'avis que la version originale et la version modifiée du document C-70 publiée pour commentaires ont servi utilement à stimuler des améliorations dans la présentation des arbres de défaillances par les titulaires de permis et à souligner le besoin d'une norme de l'ACNOR en matière d'analyse de fiabilité des systèmes liés à la sûreté des réacteurs CANDU.

Le CCSN croit aussi, toutefois, que la publication du document C-70 comme guide de réglementation, même dans sa version actuelle où les exigences réglementaires précédentes des annexes ont été modifiées en méthodes "acceptables", représente toujours un écart important par rapport à la pratique canadienne existante et aurait des répercussions qui dépasseraient la question immédiate des analyses au moyen d'arbres de défaillances. Dans son document CCSN-4 intitulé "Exigences générales de sûreté recommandées pour les centrales nucléaires" (3), le CCSN a exprimé son appui à la poursuite de la pratique en vigueur actuellement au Canada en matière de réglementation des réacteurs et ne peut donc pas appuyer d'atteinte importante à la pratique actuelle, telle la publication du document C-70 comme guide de réglementation de la CCEA.

Le CCSN reconnaît, cependant, qu'il est urgent d'établir une norme opérante pour l'analyse de fiabilité des systèmes liés à la sûreté des réacteurs CANDU et croit fermement que le meilleur moyen d'établir une telle norme est par l'entremise du Groupe de travail N290.9 existant de l'ACNOR. Le CCSN conseille donc vivement de poursuivre cette approche le plus rapidement possible, faute de quoi, la CCEA pourrait se voir forcée de publier des documents comme le document C-70 qui, selon le CCSN, porte préjudice au processus de réglementation des réacteurs nucléaires en vigueur au Canada.

RECOMMANDATIONS DU CCSN

Le Comité consultatif de la sûreté nucléaire recommande que:

1. la version actuelle du document C-70 ne soit pas publiée comme guide de réglementation.

2. la CCEA publie, comme guide de réglementation, un énoncé des principes généraux à suivre pour les analyses au moyen d'arbres de défaillances, sans mention de marche à suivre détaillée. (Toutefois, le CCSN est d'avis qu'un tel document ne serait pas nécessaire si la recommandation 4 ci-dessous est mise en vigueur prochainement.)

3. les titulaires de permis s'appliquent avec soin à résoudre les faiblesses qui subsistent dans les présentations d'arbres de défaillances, de concert avec les spécialistes de la CCEA, notamment en ce qui concerne :

a) l'identification précise des composants et de leurs modes de défaillances;

b) la clarté et la vue d'ensemble des présentations pour permettre une vérification fiable par les spécialistes de la CCEA; et

c) le retour d'information en matière d'expérience d'exploitation pour permettre la mise à jour périodique des arbres de défaillances et des calculs de risque.

4. les titulaires de permis et la CCEA accordent la plus haute priorité à la mise au point la plus rapide possible selon la marche à suivre normale d'une norme de l'ACNOR sur les analyses de fiabilité des systèmes liés à la sûreté des centrales nucléaires CANDU. La CCEA doit continuer à siéger au Groupe de travail de l'ACNOR chargé de mettre au point la norme nucléaire pour laquelle la version actuelle du document C-70 pourrait servir de données parmi d'autres.

RÉFÉRENCES

1. F.C. Boyd, Note de service au CCSN, le 3 mai 1982, "AECB Consultative Document C-70: 'Regulatory Guide on the Use of Fault Trees in Licensing Submissions' (undated)".

2. F.C. Boyd, Note de service à R.J. Atchison, le 29 novembre 1982, "ACNS Comments on C-70".

3. CCEA. CCSN. "Exigences générales de sûreté recommandées pour les centrales nucléaires", juin 1983.

ANNEXE 1

MEMBRES DU GROUPE DE TRAVAIL DU CCSN SUR LE DOCUMENT DE CONSULTATION C-70

J.T. Rogers, président
N.C. Lind
O.R. Lundell
A. Pearson

F.C. Boyd, secrétaire